Locky Strike: Smoking the Locky Ransomware Code

Floser Bacurio Jr and Rommel Joven
Anti-Virus Analysts, FortiGuard Lion Team

FORTINET®

October 7, 2016

Cryptowall

What happened to your files?
All of your files were protected by a strong encryption with RSA-2048 using CryptoWall
More information about the encryption keys using RSA-2048 can be found here: http://en.wikipedia.org/wiki/RSA_(cryptosystem)

What does this mean?
This means that the structure and data within your files have been irrevocably changed, you will not be able to work with them, read them or see them, it is the same thing as losing them forever, but with our help, you can restore them.

How did this happen?
Especially for you, on our server was generated the secret key pair RSA-2048 - public and private.
All your files were encrypted with the public key, which has been transferred to your computer via the Internet.
Decrypting of your files is only possible with the help of the private key and decrypt program, which is on our secret server.

What do I do?
Alas, if you do not take the necessary measures for the specified time then the conditions for obtaining the private key will be changed.
If you really value your data, then we suggest you do not waste valuable time searching for other solutions because they do not exist.

For more specific instructions, please visit your personal home page, there are a few different addresses pointing to your page below:

1. 3wzn5p2yiumh7akj.paypartnerstodo.com/g3tz2m
2. 3wzn5p2yiumh7akj.allepohelpto.com/g3tz2m
3. 3wzn5p2yiumh7akj.barklpaypartners.com/g3tz2m
4. 3wzn5p2yiumh7akj.maverickpaypartners.com/g3tz2m

If for some reasons the addresses are not available, follow these steps:

1. Download and install tor-browser: http://www.torproject.org/projects/torbrowser.html.en
2. After a successful installation, run the browser and wait for initialization.
3. 3wzn5p2yiumh7akj.onion/g3tz2m ◄Type in the address bar
4. Follow the instructions on the site.

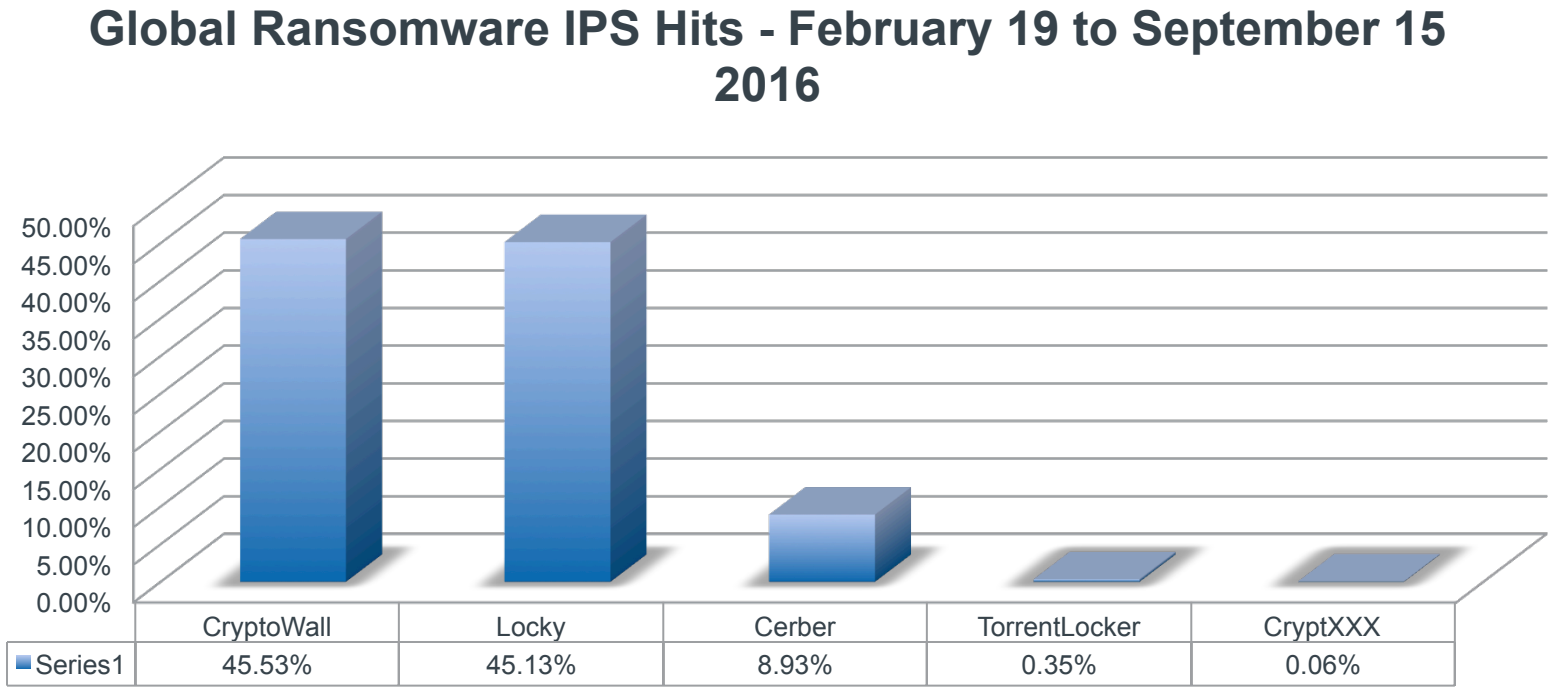
IMPORTANT INFORMATION:

paypartnerstodo.com/g3tz2m ◄Your Personal PAGE
3wzn5p2yiumh7akj.onion/g3tz2m ◄Your Personal PAGE(using TOR)
g3tz2m ◄Your personal code (if you open the site (or TOR 's) directly)

This one?

```
~==*~|||+$=$**|$_
._-~=_*-|$_*=+$||
+*+.|_|
-~*++
          !!! IMPORTANT INFORMATION !!!!

All of your files are encrypted with RSA-2048 and AES-128 ciphers.
More information about the RSA and AES can be found here:
    http://en.wikipedia.org/wiki/RSA_(cryptosystem)
    http://en.wikipedia.org/wiki/Advanced_Encryption_Standard

Decrypting of your files is only possible with the private key and decrypt program, which is on our secret server.
To receive your private key follow one of the links:
    1. http://5n7y4yihirccftc5.tor2web.org/ECCEADDE847A1F1A
    2. http://5n7y4yihirccftc5.onion.to/ECCEADDE847A1F1A

If all of this addresses are not available, follow these steps:
    1. Download and install Tor Browser: https://www.torproject.org/download/download-easy.html
    2. After a successful installation, run the browser and wait for initialization.
    3. Type in the address bar: 5n7y4yihirccftc5.onion/ECCEADDE847A1F1A
    4. Follow the instructions on the site.

!!! Your personal identification ID: ECCEADDE847A1F1A !!!
*_|$|_=
*=|~__
```

Prevalence: Global ransomware



Prevalence: Top countries

Locky Ransomware IPS Hits –
February 19 to September 15 2016

Total Hits: 36,314,789

Locky-est

US	**11,858,085**
FR	6,959,892
JP	3,071,596
KW	2,732,454
TW	1,338,216
AR	970,339
CL	890,784
PR	709,372
IT	556,602
IL	540,992

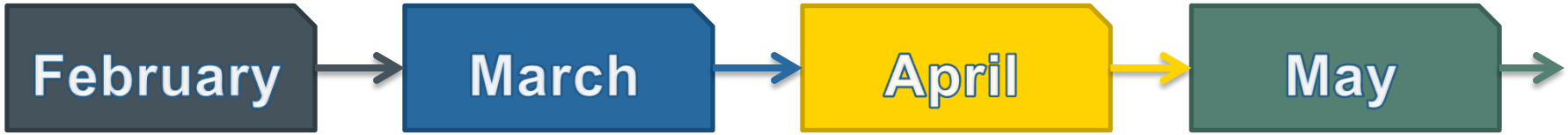
Prevalence: Affiliate program

The following is a list of affiliate methods that have been observed:

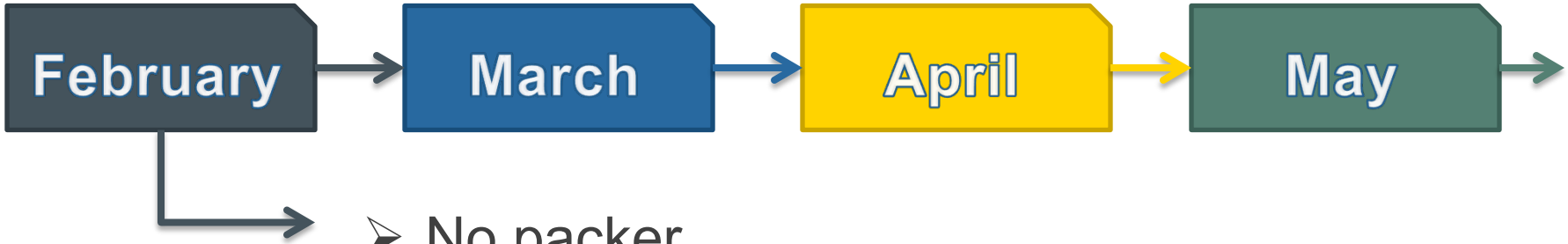
affid	Method
1	Spam email containing an attached JavaScript, MS Office Macro downloader or Windows Script File
3	Spam email containing an attached JavaScript or Microsoft Office Macro downloader
5	Spam email containing an attached JavaScript downloader
13	Compromised sites that redirects to Nuclear or Neutrino Exploit Kit
15	Spam email containing an attached JavaScript or HTA downloader

Locky Developments

Timeline of Developments: 2016



Timeline of Developments: 2016



- No packer
- “Locky” registry key
- Configuration:

```
{
AffiliateID;
ccservers;
}
```

Timeline of Developments: 2016

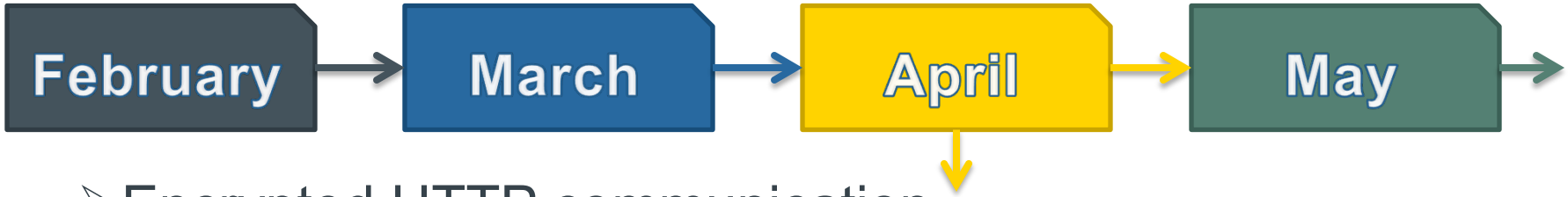
February → March → April → May

- Packed
- Registry key based on VolumeGUID
- Configuration(encrypted):

```
{
AffiliateID;
DGASeed;
delaySeconds;
FakeSvchost;
Persistence;
IgnoreRussian;
ccServers;
}
```

FORTINET

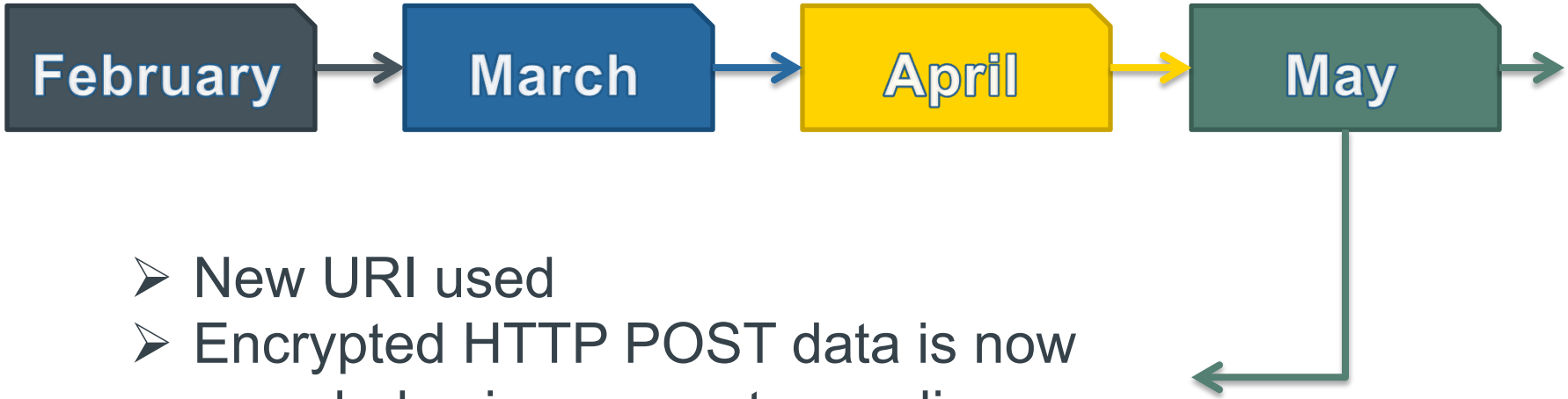
Timeline of Developments: 2016



- Encrypted HTTP communication
- Configuration:

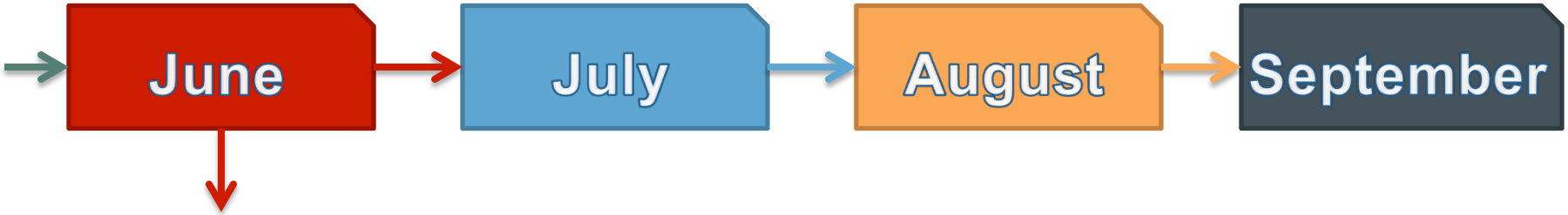
```
{
AffiliateID;
DGASeed;
delaySeconds;
FakeSvchost;
Persistence;
IgnoreRussian;
urlPath;
ccServers;
}
```

Timeline of Developments: 2016



- New URI used
- Encrypted HTTP POST data is now encoded using percent encoding

Timeline of Developments: 2016



- Requires argument. (e.g “123”, “321”)

Cracking Locky’s New Anti-Sandbox Technique

by **Floser Bacurio and Roland Dela Paz** | Jun 30, 2016 | Filed in: Security Research

The last few weeks saw new variants of the Locky ransomware that employs a new anti-sandbox technique. from its JavaScript downloader in order to decrypt embedded malicious code and execute it properly. For exa in the following manner:

sample.exe 123

Timeline of Developments: 2016

June → July → August → September

The Newest Online Threat – .Zepto Ransomware

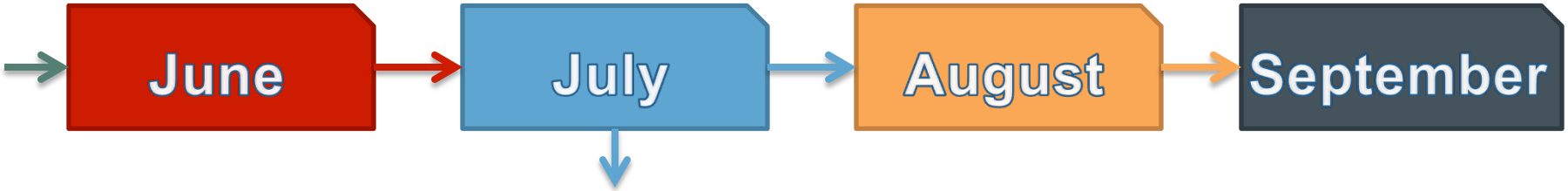
TRIPWIRE GUEST AUTHORS
JUN 29, 2016 | LATEST SECURITY NEWS

Technology CyberSecurity

Zepto ransomware spam campaign surges with over 130,000 emails in 4 days

Hackers have used subject lines like 'financial report', 'documents copy' and others in efforts to lure in victims.

Timeline of Developments: 2016



- Offline Mode encryption

PCWorld
FROM IDG

NEWS | REVIEWS | HOW-TO | VIDEO | BUSINESS | LAPTOPS | TABLETS | PHONES

Privacy | Encryption | Antivirus

Home / Security

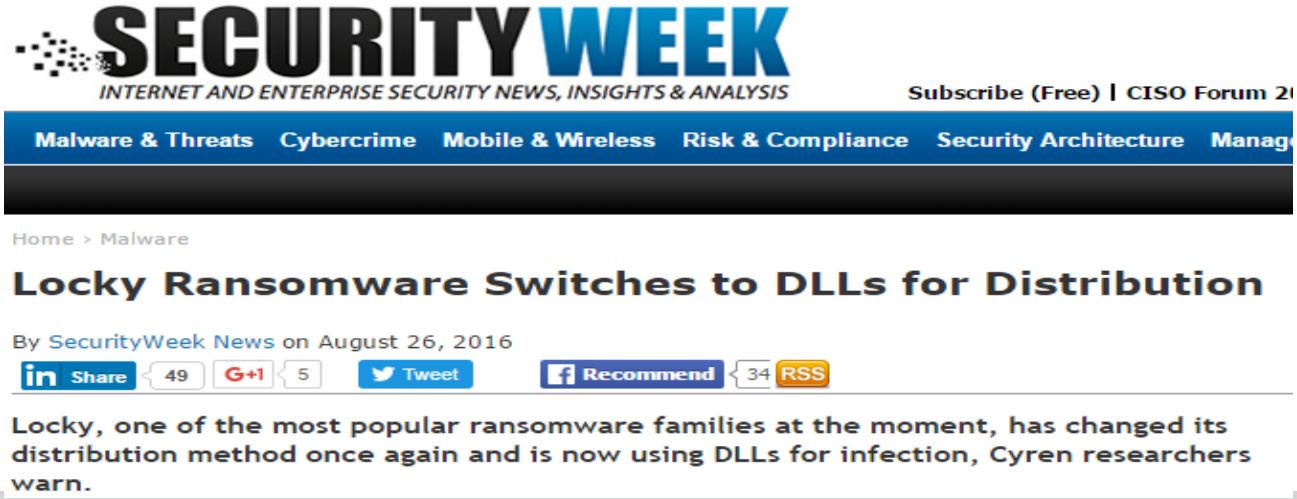
New Locky ransomware version can operate in offline mode

The program will start encrypting files even if it can't connect to a command-and-control server.

FORTINET

Timeline of Developments: 2016

June → July → August → September



SECURITY WEEK
INTERNET AND ENTERPRISE SECURITY NEWS, INSIGHTS & ANALYSIS

Subscribe (Free) | CISO Forum 2

Malware & Threats | Cybercrime | Mobile & Wireless | Risk & Compliance | Security Architecture | Manag

Home › Malware

Locky Ransomware Switches to DLLs for Distribution

By SecurityWeek News on August 26, 2016

Share 49 G+1 5 Tweet Recommend 34 RSS

Locky, one of the most popular ransomware families at the moment, has changed its distribution method once again and is now using DLLs for infection, Cyren researchers warn.

Timeline of Developments: 2016

June → July → August → September

Locky NSIS-based Ransomware

by **Floser Bacurio Jr. and Kenny Yongjian Yang** | Sep 12, 2016 | Filed in: Se

Over the last few months we saw that Locky's loader uses seed param
without the correct parameter. Afterwards, we saw Locky shift itself fror

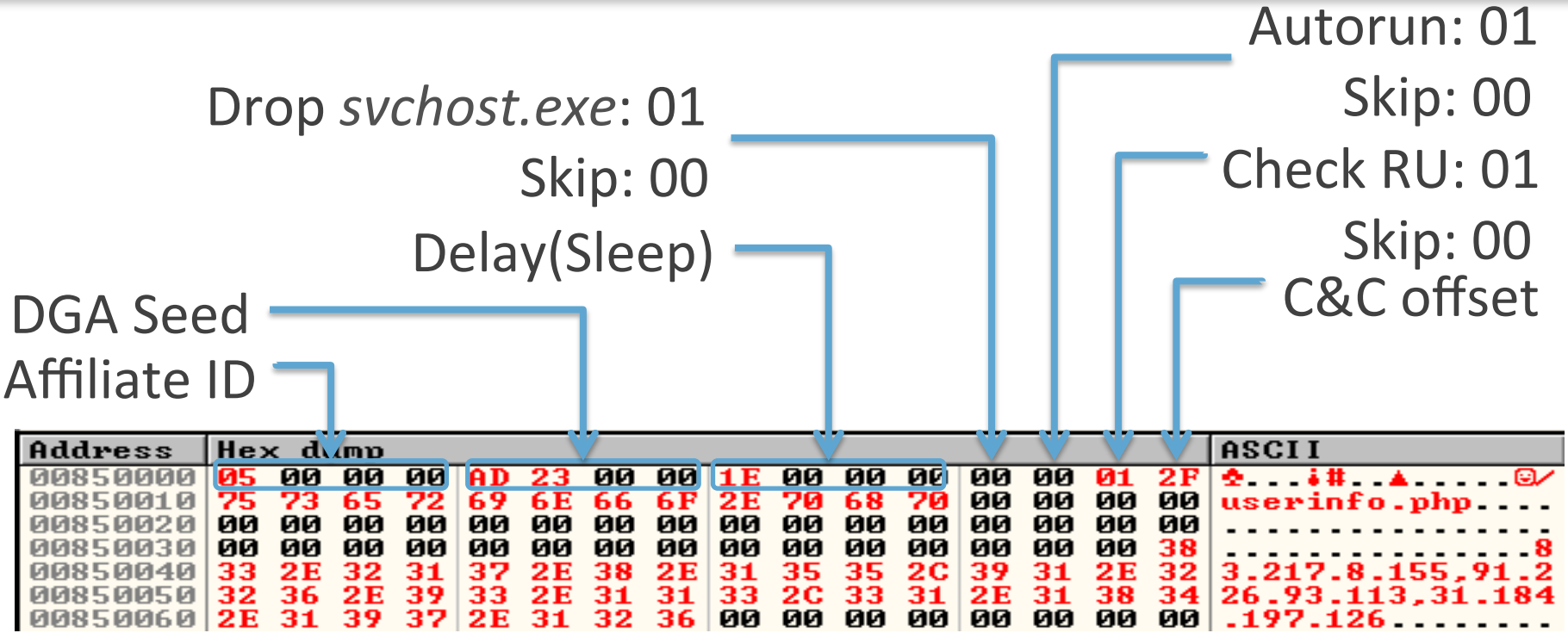
Odin File Virus Ransomware Is Here!

TRIPWIRE GUEST AUTHORS

SEP 27, 2016 | LATEST SECURITY NEWS

Technical Analysis

Configuration



Address	Hex dump																ASCII
00850000	05	00	00	00	AD	23	00	00	1E	00	00	00	00	00	01	2F	♣...¡#..▲.....☺/
00850010	75	73	65	72	69	6E	66	6F	2E	70	68	70	00	00	00	00	userinfo.php....
00850020	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	....
00850030	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	38	8
00850040	33	2E	32	31	37	2E	38	2E	31	35	35	2C	39	31	2E	32	3.217.8.155,91.2
00850050	32	36	2E	39	33	2E	31	31	33	2C	33	31	2E	31	38	34	26.93.113,31.184
00850060	2E	31	39	37	2E	31	32	36	00	00	00	00	00	00	00	00	.197.126........

FORTINET

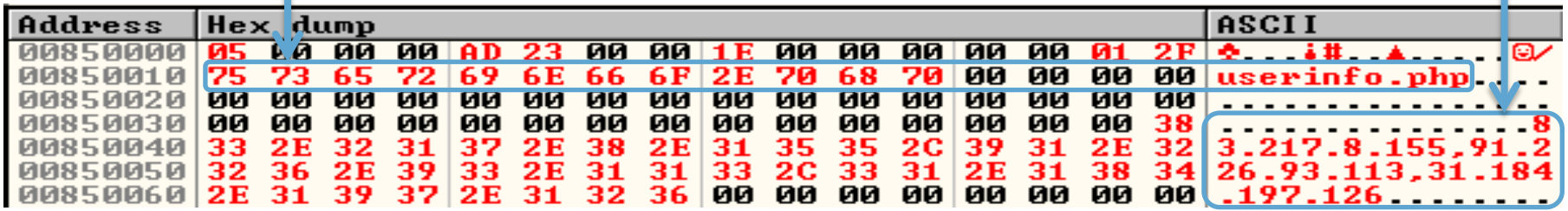
Configuration

URI for its C&C

- main.php
- submit.php
- userinfo.php
- access.cgi

C&Cs

- /upload/_dispatch.php
- /php/upload.php
- /data/info.php
- /apache_handler.php



Address	Hex dump	ASCII
00850000	05 00 00 00 AD 23 00 00 1E 00 00 00 00 00 01 2F	♣....¡#..▲.....☺/
00850010	75 73 65 72 69 6E 66 6F 2E 70 68 70 00 00 00 00	userinfo.php....
00850020	00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00	....
00850030	00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 38	8
00850040	33 2E 32 31 37 2E 38 2E 31 35 35 2C 39 31 2E 32	3.217.8.155,91.2
00850050	32 36 2E 39 33 2E 31 31 33 2C 33 31 2E 31 38 34	26.93.113,31.184
00850060	2E 31 39 37 2E 31 32 36 00 00 00 00 00 00 00 00	.197.126........

Configuration

Address	Hex dump	ASCII
00850000	05 00 00 00 AD 23 00 00 1E 00 00 00 00 00 01 2F	♣...¡#..▲.....☺/
00850010	75 73 65 72 69 6E 66 6F 2E 70 68 70 00 00 00 00	userinfo.php....
00850020	00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00	....
00850030	00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 38	8
00850040	33 2E 32 31 37 2E 38 2E 31 35 35 2C 39 31 2E 32	3.217.8.155,91.2
00850050	32 36 2E 39 33 2E 31 31 33 2C 33 31 2E 31 38 34	26.93.113,31.184
00850060	2E 31 39 37 2E 31 32 36 00 00 00 00 00 00 00 00	.197.126........

Configuration: Offline

Online mode

Address	Hex dump																ASCII
00850000	05	00	00	00	AD	23	00	00	1E	00	00	00	00	00	01	2F	♣...¡#..▲.....☺/
00850010	75	73	65	72	69	6E	66	6F	2E	70	68	70	00	00	00	00	userinfo.php....
00850020	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	....
00850030	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	38	8
00850040	33	2E	32	31	37	2E	38	2E	31	35	35	2C	39	31	2E	32	3.217.8.155,91.2
00850050	32	36	2E	39	33	2E	31	31	33	2C	33	31	2E	31	38	34	26.93.113,31.184
00850060	2E	31	39	37	2E	31	32	36	00	00	00	00	00	00	00	00	.197.126........

No DGA Seed

No C&C offset

Offline mode

Address	Hex dump																ASCII
019A0000	03	00	00	00	00	00	00	00	27	00	00	00	00	00	01	00	♥.......'.....☺.
019A0010	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	....
019A0020	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	....
019A0030	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	....
019A0040	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	....
019A0050	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	....
019A0060	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	....

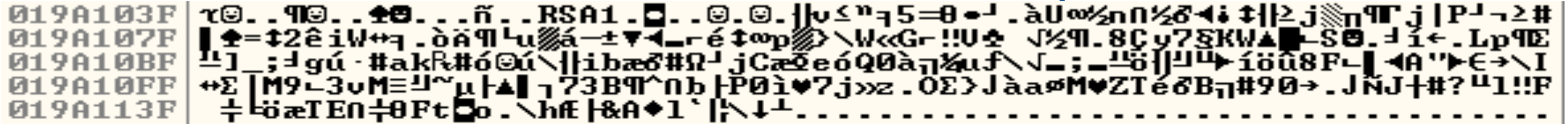
No C&Cs and URI

Configuration: Offline

Offline mode

Address	Hex dump																ASCII
019A0000	03	00	00	00	00	00	00	00	27	00	00	00	00	00	01	00	♥.......'......☺.
019A0010	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	....
019A0020	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	....
019A0030	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	....
019A0040	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	....
019A0050	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	....
019A0060	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	....

Embedded Public RSA key



Configuration: Offline

Embedded Ransom Text

```
019A1493 ∩ππ.~.=¦*_=~..-$¦$*¦.~.$_..              !!! IMPORTANT INFORMATION
019A14D3  !!!!....All of your files are encrypted with RSA-2048 and AES-1
019A1513 28 ciphers...More information about the RSA and AES can be found
019A1553  here:..     http://en.wikipedia.org/wiki/RSA_(cryptosystem)..
019A1593  http://en.wikipedia.org/wiki/Advanced_Encryption_Standard..
019A15D3 ..Decrypting of your files is only possible with the private key
019A1613  and decrypt program, which is on our secret server...To receive
019A1653  your private key follow one of the links:..      1. http://5n7y4y
019A1693 ihirccftc5.tor2web.org/FF00000000000000FF..      2. http://5n7y4yihi
019A16D3 rccftc5.onion.to/FF00000000000000FF....If all of this addresses ar
019A1713 e not available, follow these steps:..      1. Download and instal
019A1753 l Tor Browser: https://www.torproject.org/download/download-easy
019A1793 .html..     2. After a successful installation, run the browser a
019A17D3 nd wait for initialization...      3. Type in the address bar: 5n7
019A1813 y4yihirccftc5.onion/FF00000000000000FF..      4. Follow the instruct
019A1853 ions on the site.....!!! Your personal identification ID: FF0000
019A1893 00000000FF !!!....~+_..==-_¦-..¦=+-¦-_¦*~*..==-~~...............
```

Embedded HTML Ransom Text

```
019A37BE <a href="http://5n7y4yihirccftc5.tor2web.org/FF00000000000000FF" t
019A37FE arget="_blank">http://5n7y4yihirccftc5.tor2web.org/FF000000000000
019A383E 0FF</a><br /><span class='kqfldfq'> </span><div class=owfbp
019A387E rnjid>qqsiz</div><span class='kqfldfq'>a</span><span class='kqfl
019A38BE dfq'>c</span><div class=owfbprnjid>wmdidtjxu</div><span class='k
019A38FE qfldfq'> </span><div class=owfbprnjid>bkzqxn</div>2.<span class=
```


FORTINET

Victim ID: Online

Locky creates a victim ID that needs to identify unique systems.

The victim ID is created from the following information:

- Volume GUID of the *WindowsDirectory*
- *MD5* hash of the GUID value

e.g. ***victim_ID = 4DF383039AB03953***

Victim ID: Offline

The victim ID is created from the following information:

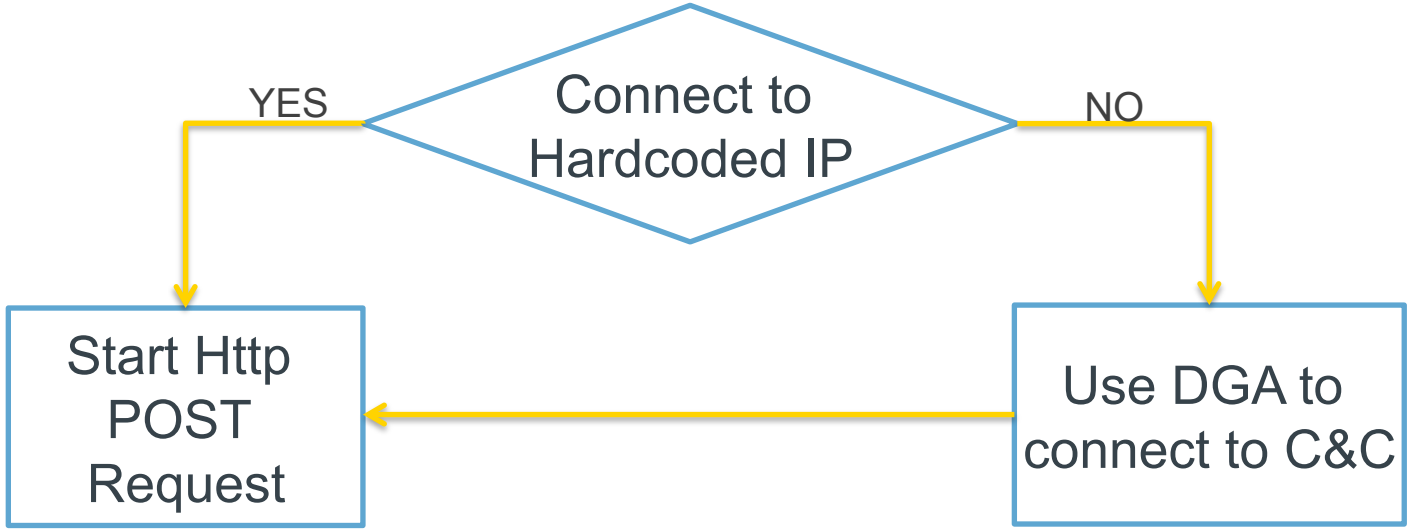
- GUID of the *WindowsDirectory*
- Default UI *Language*
- *OS* version
- Domain Controller
- *Affiliate ID* from the configuration
- *Public key ID* from the configuration

Encodes it using a hard coded 32 character value:
"**YBNDRFG8EJKMCPQX0T1UWISZA345H769**".

e.g. ***victim_ID = IZ8FDGTNEN85I7JZ***

C&C Communication

Communication Protocol: C&C



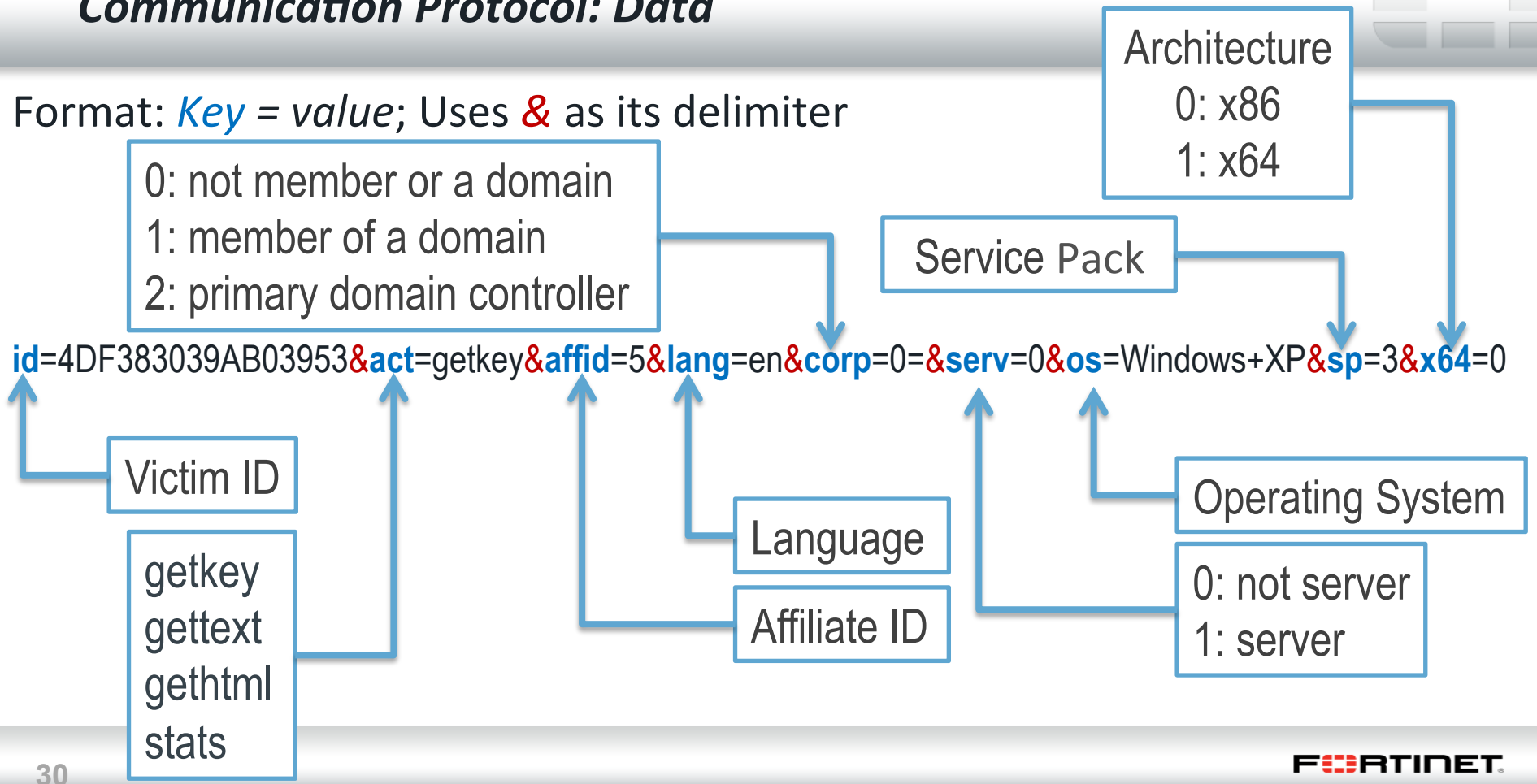
Communication Protocol: Data

Format: *Key* = *value*; Uses *&* as its delimiter

id=4DF383039AB03953**&act**=getkey**&affid**=5**&lang**=en**&corp**=0=**&serv**=0**&os**=Windows+XP**&sp**=3**&x64**=0

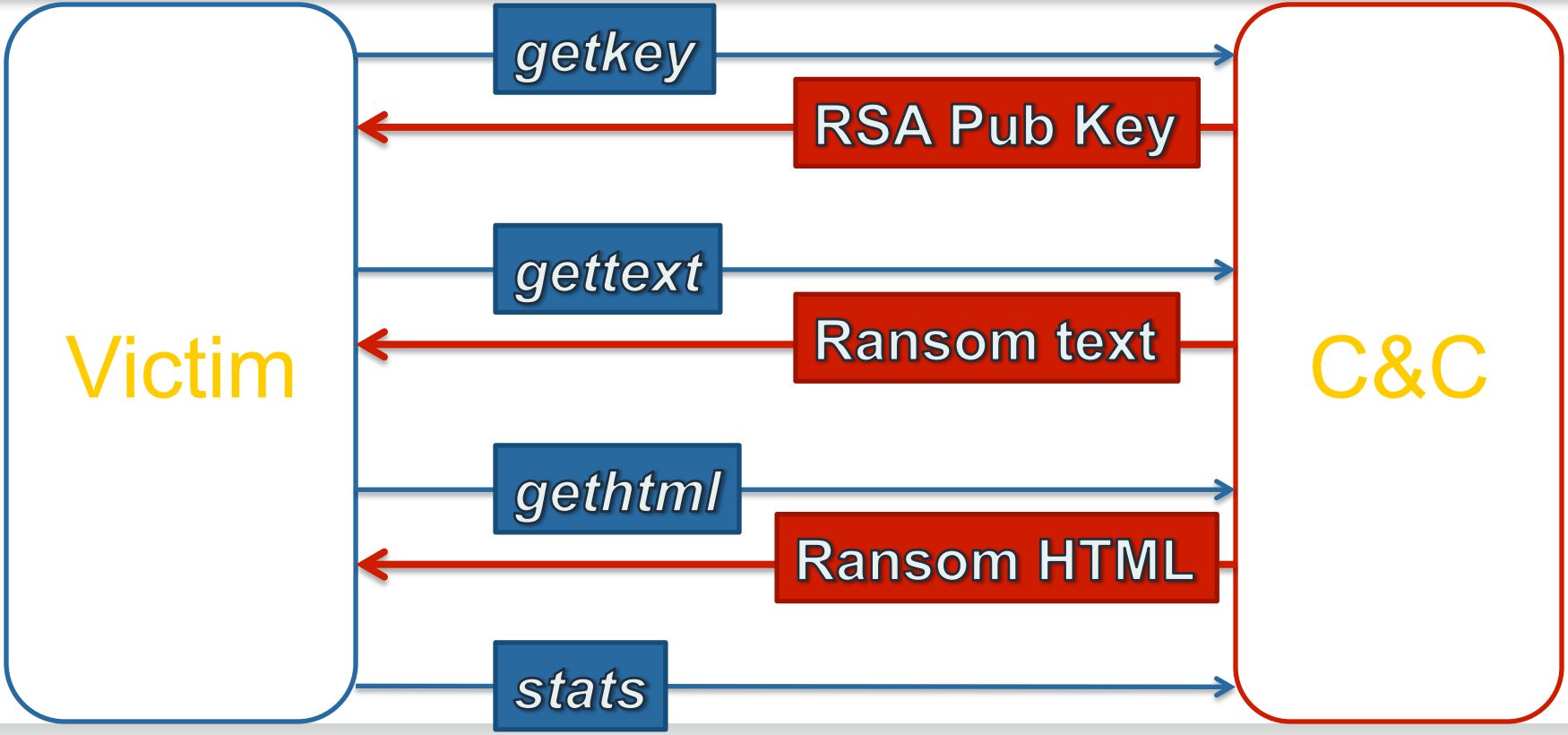
Communication Protocol: Data

Format: *Key* = *value*; Uses & as its delimiter



FORTINET

Communication Protocol: Http request



File Encryption

File Encryption: Targeted drives

- Drive_Removable
- Drive_Fixed
- Drive_Remote
- Drive_Ramdisk

File Encryption: Targeted extensions

Total of **194** file extensions:

.n64, .m4a, .m4u, .m3u, .mid, .wma, .flv, .3g2, .mkv, .
*3gp, .mp4, .mov, .avi, .asf, .mpeg, .vob, .mpg, .wmv, .fla, .swf, .wav, .mp3, .qcow2, .vdi, .vmdk, .vmx, .**wallet**, .upk, .sav, .re4, .ltx, .litesql, .litemod, .lbf, .iwi, .forge, .das, .d3dbsp, .bsa, .bik, .asset, .apk, .gpg, .aes, .ARC, .PAQ, .tar, .bz2, .tbk, .bak, .tar, .tgz, .gz, .*
*7z, .rar, .zip, .djv, .djvu, .svg, .bmp, .png, .gif, .raw, .cgm, .jpeg, .jpg, .tif, .tiff, .NEF, .psd, .cmd, .bat, .sh, .class, .jar, .java, .rb, .asp, .cs, .brd, .sch, .dch, .dip, .pl, .vbs, .vb, .js, .h, .asm, .pas, .cpp, .c, .php, .ldf, .**mdf**, .ibd, .MYI, .MYD, .frm, .odb, .dbf, .db, .mdb, .**sql**, .**SQLITEDB**, .SQLITE3, .011, .010, .009, .008, .007, .006, .005, .004, .003, .002, .*
001, .pst, .onetoc2, .asc, .lay6, .lay, .ms11(Securitycopy), .ms11, .sldm, .sldx, .ppsm, .ppsx, .ppam, .docb, .mml, .sxm, .otg, .odg, .uop, .potx, .potm, .pptx, .pptm, .std, .sxd, .pot, .pps, .sti, .sxi, .otp, .odp, .wb2, .
*123, .wks, .wk1, .xltx, .xltm, .**xlsx**, .xlsm, .xlsb, .slk, .xlw, .xlt, .xlm, .xlc, .dif, .stc, .sxc, .ots, .ods, .**hwp**, .*
*602, .dotm, .dotx, .docm, .**docx**, .DOT, .3dm, .max, .*
*3ds, .xml, .txt, .**CSV**, .uot, .RTF, .**pdf**, .XLS, .PPT, .stw, .sxw, .ott, .odt, .**DOC**, .pem, .p12, .csr, .crt, .key,* ***wallet.dat***

File Encryption: Targeted extensions

From **194** to **460** file extensions:

*.yuv, .qbx, .ndd, .exf, .cdr4, .vmsd, .dat, .indd, .pspimage, .obj, .ycbcra, .qbw, .mrw, .erf, .cdr3, .vhdx, .cmt, .iif , .ps, .mlb, .xis, .qbr, .**moneywell**, .erbsql, .bpw, .vhd, .bin, .fpx, .pct, .md, .x3f, .qba, .mny, .eml, .bgt, .vbox, . aiff, .fff, .pcd, .mbx, .x11, .py, .mmw, .dxg, .bdb, .stm, .xlk, .fdb, .m4v, .lit, .wpd, .**psafe3**, .mfw, .drf, .bay, .st7, .wad, .dtd, .m, .laccdb, .tex, .plc, .mef, .dng, .bank, .rvt, .tlg, .design, .fxg, .kwm, .sxg, .plus_muhd, .mdc, .dgc, .**backupdb**, .qcow, .st6, .ddd, .flac, .idx, .stx, .pdd, .lua, .des, .backup, .qed, .st4, .dcr, .eps, .html, .st8, .p7c, . kpdx, .der, .back, .pif, .say, .dac, .dxb, .flf, .st5, .p7b, .kdc, .ddrw, .awg, .pdb, .sas7bdat, .cr2, .drw, .dxf, .srw, . oth, .kdbx, .**ddoc**, .apj, .pab, .qbm, .cdx, .**db3**, .dwg, .srf, .orf, .kc2, .dcs, .ait, .ost, .qbb, .cdf, .cpi, .dds, .sr2, .o dm, .jpe, .dc2, .agdl, .ogg, .ptx, .blend, .cls, .css, .sqlite, .odf, .incpas, .db_journal, .ads, .nvram, .pfx, .bkp, .cd r, .**config**, .sdf, .nyf, .iiq, .csl, .adb, .ndf, .pef, .al, .arw, .cfg, .sda, .nxl, .ibz, .csh, .acr, .m4p, .pat, .adp, .ai, .cer , .sd0, .nx2, .**ibank**, .crw, .ach, .m2ts, .oil, .act, .aac, .asx, .s3db, .nwb, .hbk, .craw, .accdt, .log, .odc, .xlr, .thm , .aspx, .rwz, .ns4, .gry, .cib, .accdr, .hpp, .nsh, .xlam, .srt, .aoi, .rwl, .ns3, .grey, .ce2, .accde, .hdd, .nsg, .xla, .save, .accdb, .rdb, .ns2, .gray, .ce1, .ab4, .groups, .nsf, .wps, .**safe**, .**7zip**, .rat, .nrw, .fhd, .cdrw, . 3pr, .flvv, .nsd, .tga, .rm, .1cd, .raf, .nop, .fh, .cdr6, . 3fr, .edb, .nd, .rw2, .pwm, .wab, .qby, .nk2, .ffd, .cdr5, .vmxf, .dit, .mos, .r3d, .pages, .prf, .oab, .msg, .mapima il, .jnt, .dbx, .contact*

File Encryption: Algorithm

Encryption used:

- Uses both RSA and AES algorithms
- The AES-128 key is randomly generated for each file
- The AES-128 key is used to encrypt the file and it's filename
- After encryption, the AES-128 key will be encrypted by RSA-2048

File Encryption: Filename

Format of filenames of encrypted files.

4DF383039AB03953D81660EB4CADC28D.locky

Victim ID File ID

File Encryption: Filename

Format of filenames of encrypted files.

4DF383039AB03953D81660EB4CADC28D.locky

Victim ID File ID

0X3U7IYC-IA09-CQ94-D26F-CFA67B8E895D.zepto

Victim ID File ID

File Encryption: Filename

Format of filenames of encrypted files.

4DF383039AB03953D81660EB4CADC28D.locky

Victim ID File ID

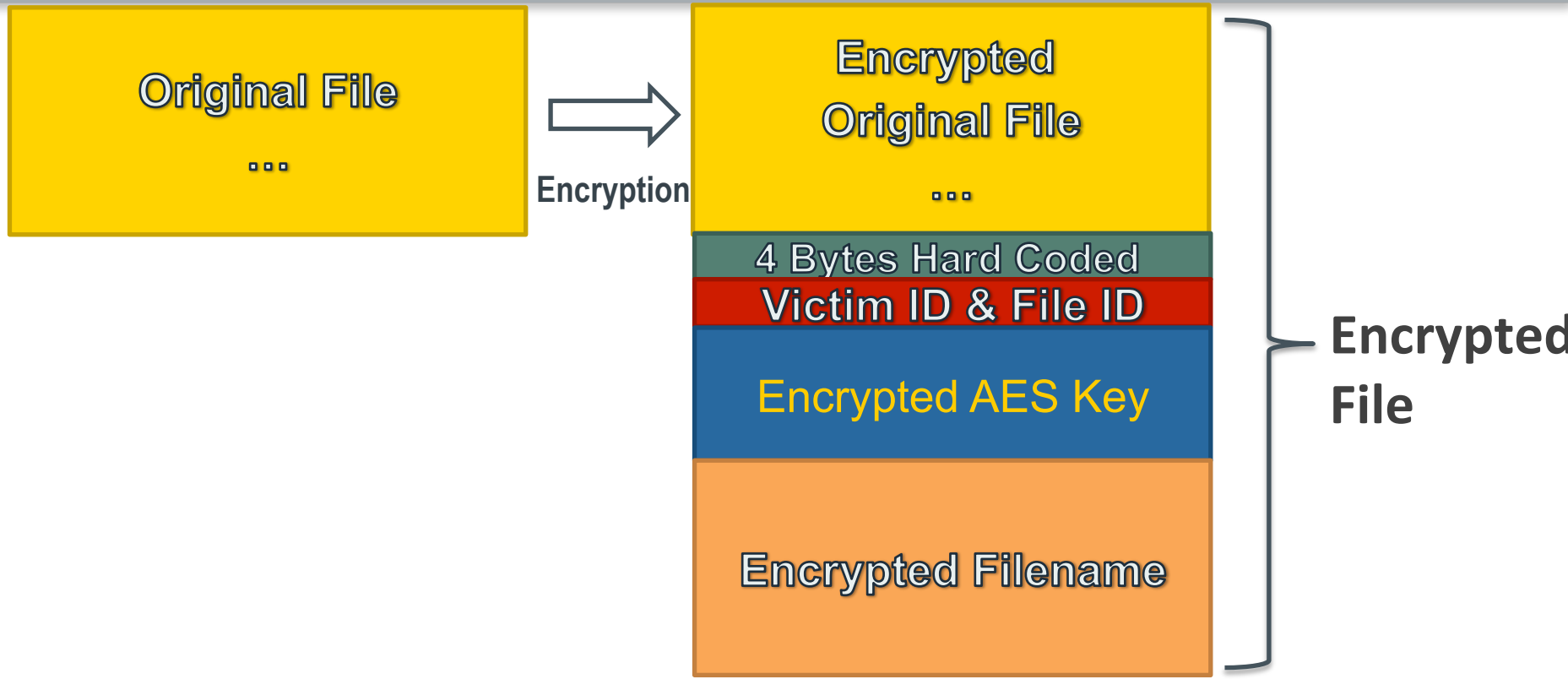
0X3U7IYC-IA09-CQ94-D26F-CFA67B8E895D.zepto

Victim ID File ID

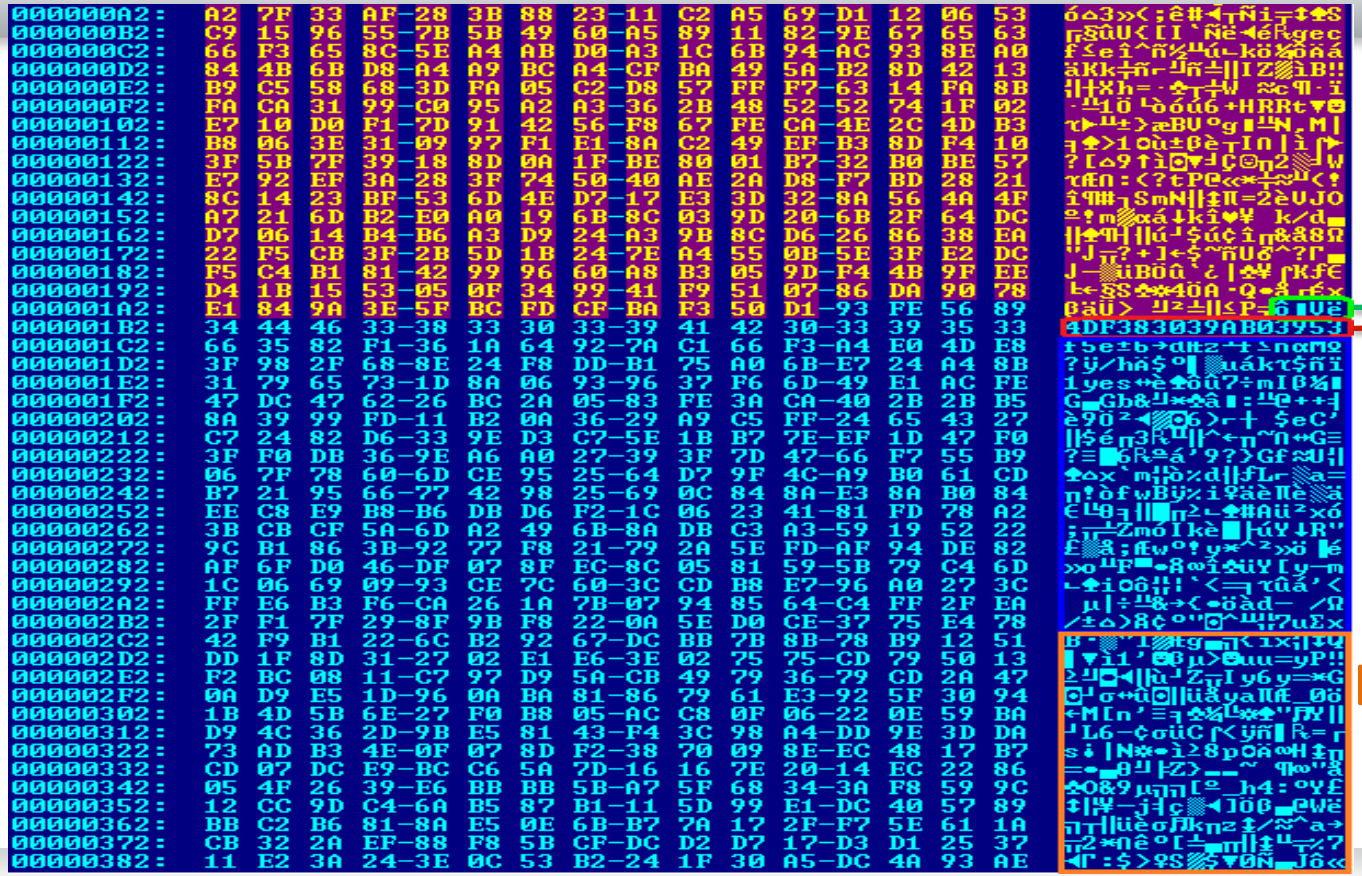
0X3U7IYC-IA09-CQ94-D26F-CFA67B8E895D.odin

Victim ID File ID

File Encryption: File layout



File Encryption: File layout



Encrypted Data

*Encryption used:
AES-128

Hardcoded Value

Victim ID & File ID

Encrypted AES Key

*Encryption used:
RSA-2048

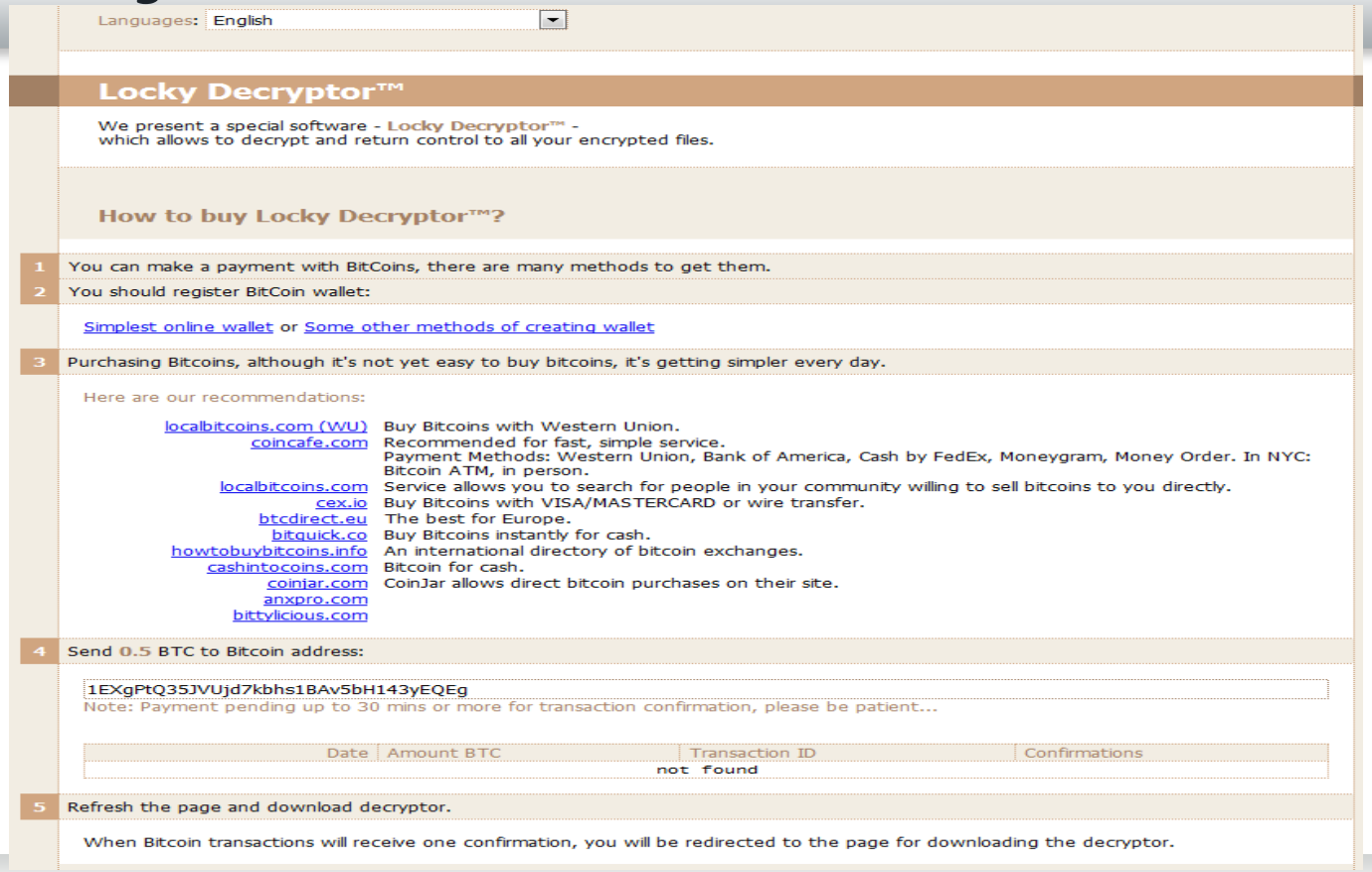
Encrypted Filename

*Encryption used:
AES-128

HTML Ransom Note

```
ï»¿|.=+ =+$-=..-.__=
=.-..$$|= $$=+*
            !!! IMPORTANT INFORMATION !!!!

All of your files are encrypted with RSA-2048 and AES-128 ciphers.
More information about the RSA and AES can be found here:
    http://en.wikipedia.org/wiki/RSA_(cryptosystem)
    http://en.wikipedia.org/wiki/Advanced_Encryption_Standard

Decrypting of your files is only possible with the private key and decrypt program, which is on our secret server.
To receive your private key follow one of the links:
    1. http://5n7y4yihirccftc5.tor2web.org/ECCEADDE847A1F1A
    2. http://5n7y4yihirccftc5.onion.to/ECCEADDE847A1F1A

If all of this addresses are not available, follow these steps:
    1. Download and install Tor Browser: https://www.torproject.org/download/download-easy.html
    2. After a successful installation, run the browser and wait for initialization.
    3. Type in the address bar: 5n7y4yihirccftc5.onion/ECCEADDE847A1F1A
    4. Follow the instructions on the site.

!!! Your personal identification ID: ECCEADDE847A1F1A !!!
*+$-==+=+_
_ + .+--. ..|++=$-=+
```

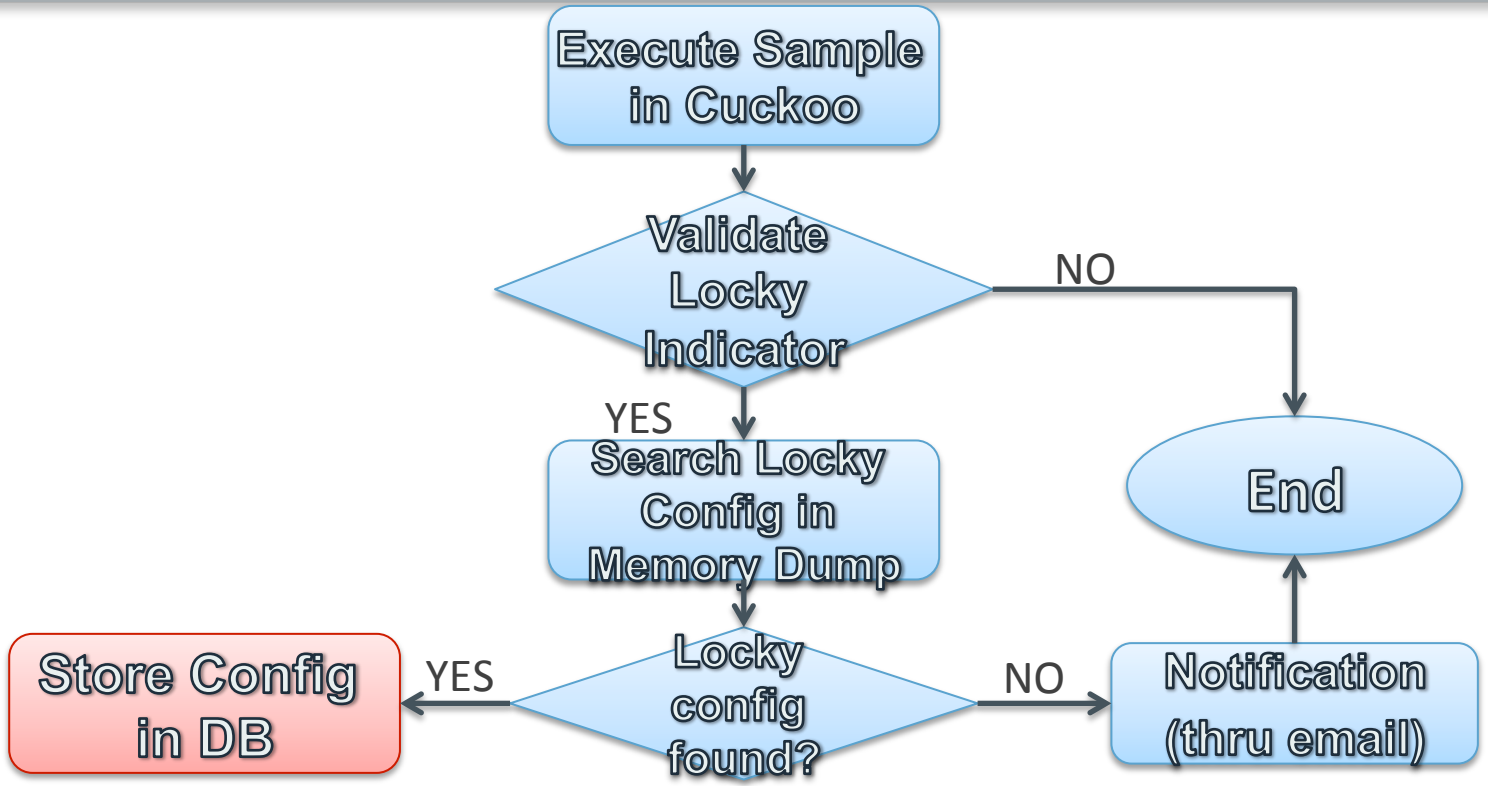
Decryptor Page



Harvest Locky Configuration

Automate Configuration Extraction: Overview

Cuckoo Setup



Demo: Locky Config Extraction in Cuckoo Sandbox

Takeaways

Thank you

fbacurio@fortinet.com
rjoven@fortinet.com

@fbacurio
@rommeljoven17